

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-265582

**(43)Date of publication of application : 28.09.2001**

G06F 9/06  
G06F 12/14

(71)Applicant : HONDA MOTOR CO LTD

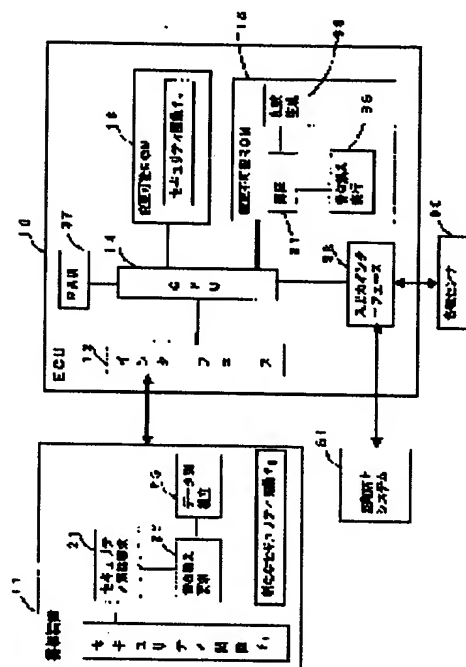
(72)Inventor : YASHIKI TETSUYA  
MATSUURA MASANORI  
MIZUO NAHIKO

## (54) MEMORY REWRITING SYSTEM FOR VEHICLE CONTROLLER

**(57)Abstract:**

**PROBLEM TO BE SOLVED:** To prevent illegal rewriting by rewriting information concerning security stored in the memory of a vehicle controller.

**SOLUTION:** This memory rewriting system for vehicle controller is mounted to the vehicle controller and provided with a memory area where erasing and writing is possible and the first security information for judging rewriting permission to the memory area is stored, a rewriting device for transferring the second security information to the vehicle controller from outside, and a rewriting means, mounted on the vehicle controller, for erasing the first security information and writing the second security information transferred from the rewriting device. Since information for realizing a rewriting security function can be rewritten, the security function can be restored even when the information is known to the third party. Furthermore, the rewriting system can operate in cooperation with a burglarproof system.



## LEGAL STATUS

[Date of request for examination] 27.11.2003

[Date of sending the examiner's decision of rejection] 30.01.2007

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

**[Date of final disposal for application]**

[Patent number] 3954271

[Date of registration] 11.05.2007

|   |             |
|---|-------------|
| [Number of appeal against examiner's decision of rejection] | 2007-006113 |
|---|-------------|

[Date of requesting appeal against examiner's decision 28.02.2007 of rejection]

[Date of extinction of right]

(43)公開日 平成13年9月28日(2001.9.28)

|       |       |  |         |           |          |
|-------|-------|--|---------|-----------|----------|
| F I   |       |  |         |           | データ*(参考) |
| C O F | 9/06  |  | S S O J | 5 B 0 1 7 |          |
|       |       |  | S 4 O M | 5 B 0 7 6 |          |
|       | 12/14 |  | 3 1 0 D |           |          |

審査請求 未請求 請求項の数 4 O L (全 11 頁)

(71)出願人 00000:326  
本田技研工業株式会社  
東京都港区南青山二丁目1番1号

(72)発明者 屋敷 哲也  
埼玉県和光市中央1丁目4番1号 株式会社  
社本田技術研究所内

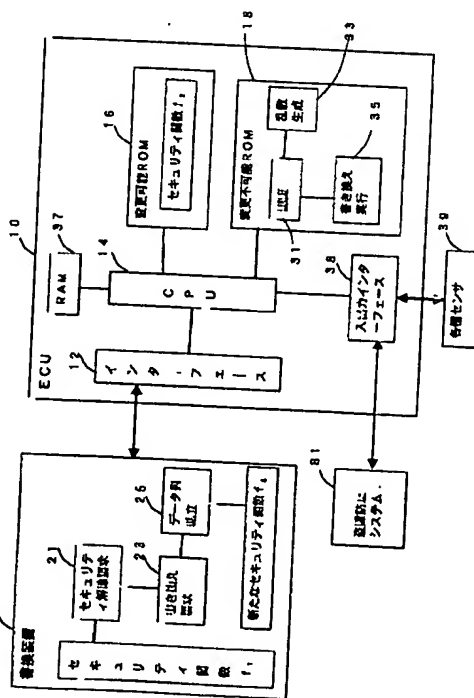
(72)発明者 松浦 正典  
埼玉県和光市中央1丁目4番1号 株式会社  
社本田技術研究所内

(74)代理人 100081721  
弁理士 岡田 次生

(54) 【発明の名称】 車両制御装置のためのメモリ書き換えシステム

【課題】車両制御装置のメモリに格納されたセキュリティに関する情報を書き換えることができるようにし、不正の書き換えを防止する。

【解決手段】車両制御装置に搭載され、消去および書き込みが可能なメモリ領域であって、該メモリ領域に対する書き換え許可を判断する第1のセキュリティ情報を格納するメモリ領域と、車両制御装置に第2のセキュリティ情報を外部から転送する書き換え装置と、車両制御装置に搭載され、前記第1のセキュリティ情報を消去して、書き換え装置から転送された第2のセキュリティ情報を書き込む書き換え手段とを備える、車両制御装置のための書き換えシステムを提供する。書き換えのセキュリティ機能を実現する情報を書き換えることができるので、該情報が第三者に知られてしまった場合でも、セキュリティ機能を回復させることができる。また、書き換えシステムは、盗難防止システムと協調して動作することができる。



## 【特許請求の範囲】

【請求項1】車両制御装置に搭載され、消去および書き込みが可能なメモリ領域であって、該メモリ領域に対する書き換え許可を判断する第1のセキュリティ情報を格納するメモリ領域と、

前記車両制御装置に第2のセキュリティ情報を外部から転送する書き換え装置と、

前記車両制御装置に搭載され、前記第1のセキュリティ情報を消去して、前記書き換え装置から転送された第2のセキュリティ情報を書き込む書き換え手段と、  
を備える車両制御装置のためのメモリ書き換えシステム。

【請求項2】前記第2のセキュリティ情報の書き込みがプログラムによって実行され、該プログラムが、前記車両制御装置に搭載された消去および書き込みが不可能なメモリ領域に格納されている請求項1に記載の車両制御装置のためのメモリ書き換えシステム。

【請求項3】前記第2のセキュリティ情報が、前記書き換え装置によって任意に設定される請求項1または請求項2に記載の車両制御装置のためのメモリ書き換えシステム。

【請求項4】前記第1のセキュリティ情報による書き換え許可が、盗難防止システムによって車両動作が許可された場合に書き換えが許可される請求項1から請求項3のいずれかに記載の車両制御装置のためのメモリ書き換えシステム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、車載制御装置のメモリに保存されたプログラムを、外部の書き換え装置から転送される別のプログラムに書き換えるメモリ書き換えシステムに関する。

## 【0002】

【従来の技術】現在、車両は、搭載された複数の電子制御ユニット（以下、「ECU」という）により、空燃比、燃料噴射量、エミッションなどのエンジンに関する制御、パワーウィンドウ、エアバッグ、ABSなどの車体に関する制御など、様々に制御されている。ECUは、車両に搭載された様々なセンサによって感知された車両の現在の状態および走行状況に基づいて、車両を様々に制御する。

【0003】一方、車両に盗難防止システムが搭載されることがある。多くの盗難防止システムは、運転者がエンジン始動時に使用したイグニッションキーが正規のものを電子的に判定し、正規のイグニッションキーと判定したならば、車両動作を許可する信号をECUに転送する。ECUは、その許可信号を受信するまで、燃料噴射を停止するなどの手法によりエンジンを始動させないようにする。したがって、正規のイグニッションキーではないと判定された場合には、不正な運転者とみなされ、車

両を動かすことができない。

【0004】ECUは、中央演算処理装置（CPU）、実行するプログラムおよびデータを格納するROM（読み取り専用メモリ）、実行時の作業領域を提供し演算結果などを記憶するRAM（ランダムアクセスメモリ）、各種センサからの信号を受け取り、およびエンジン各部に制御信号を送る入出力インターフェースを備えている。

【0005】上記ROMに、フラッシュメモリ、EEPROM、EPROMのような消去および書き込みが可能なROMを使用して、必要に応じてプログラムを書き替えることが行われている。特開昭63-223901号公報には、外部装置からの要求によって、ECUを車両に搭載したままで、ECUのEEPROMに格納されたプログラムを変更する方法が記載されている。

【0006】通常、ECUのROMに格納されたプログラムを変更する機能には、外部装置からのアクセスに対してセキュリティがかけられており、ユーザーおよびその他の第三者がROMに格納されたプログラムおよびデータを不正に書き換えることを防止している。特開平3-238541号公報には、ROMに格納されたデータに基づくチェックデータを予め記憶しておき、車両の出荷後、ECUが所定のタイミングでROMに格納されたデータに基づく新たなチェックデータを作成し、予め記憶されたチェックデータと比較して、一致していなければデータの改ざんが行われたと判断し、警告灯を点灯させる車両制御装置が記載されている。

【0007】上記のセキュリティを解除する「キー（Key）」は、自動車メーカーと契約した書き換え装置メーカーにのみ公開されている。したがって、その自動車メーカーによって認可された書き換え装置メーカーの書き換え装置のみが、「キー」を使用してその自動車のECUのROMに格納されたデータを変更することができる。

【0008】プログラムの典型的な変更手順を簡単に述べると、上記の「キー」は、通常何らかの関数で表され、書き換え装置およびECUに同じものが用意されている。書き換え装置をECUに接続し、書き換え装置は、自身が持っている関数（キー）を使用して、ECUから送信された任意の数値に対する関数値を算出し、該関数値をECUに送信する。同時に、ECUも、自身が持っている関数（キー）を使用してその数値に対する関数値を求める。ECUは、書き換え装置から受信された関数値と、自身が求めた関数値とを比較し、一致すればセキュリティを解除する。こうして、書き換え装置は、ROMに格納されたデータを書き換えることを許可される。一致しなければ、書き換え装置とECUの持つ関数（キー）が異なっており、書き換え装置は正規のものではないと判断されてセキュリティは解除されず、書き換え装置はROMに格納されたデータを書き換えることは

できない。

【0009】

【発明が解決しようとする課題】しかし、従来、セキュリティを解除するキーは、ECUに搭載されたROMの変更不能なメモリ領域に格納されており、車両が出荷された後に書き換え装置を使用して変更することはできなかった。このため、万が一このキーがユーザーおよびその他の第三者に知られてしまった場合、正規の書き換え装置でなくてもROMのデータを書き換えることができるようになり、セキュリティが機能しなくなるという事態が生じる。

【0010】一方、車両に盗難防止システムが搭載されている場合、盗難防止システムを稼働するのに使用されるプログラムが書き換えられると、盗難防止システムが無効化されるおそれがある。したがって、ROMに格納されたデータおよびプログラムを書き換えるシステムには、盗難防止システム以上のセキュリティが要求される。

【0011】この発明は、上記の問題点を解決するものであり、その目的は、車両の出荷後においても、ECUのROMに格納されたプログラムまたはデータの改ざんを防止するセキュリティを解除するためのキーを変更することができる車両制御装置のためのメモリ書き換えシステムを提供することである。こうして、キーがメーカー以外の第三者に知られてしまった場合でも、書き換え装置によってメーカーがキーを変更することができるので、セキュリティ機能を容易に回復させることができる。

【0012】この発明の他の目的は、盗難防止システムと協調して動作することができる車両制御装置のためのメモリ書き換えシステムを提供することである。こうすることにより、盗難防止システムと協調したセキュリティ機能を確保することができる。

【0013】

【課題を解決するための手段】上記の課題を解決するため、請求項1の車両制御装置のためのメモリ書き換えシステムは、車両制御装置に搭載され、消去および書き込みが可能なメモリ領域であって、該メモリ領域に対する書き換え許可を判断する第1のセキュリティ情報を格納するメモリ領域と、前記車両制御装置に第2のセキュリティ情報を外部から転送する書き換え装置と、前記車両制御装置に搭載され、前記第1のセキュリティ情報を消去して、前記書き換え装置から転送された第2のセキュリティ情報を書き込む書き換え手段とを備えるという構成をとる。

【0014】請求項1の発明によると、車両制御装置のメモリに記憶された情報が不正に書き換えられることを防止する書き換え許可を判断するセキュリティ情報が第三者に知られてしまった場合でも、書き換え装置によりこのセキュリティ情報を変更することができるので、不

正なメモリ書き換えの拡大を防止することができる。

【0015】請求項2の発明は、請求項1の車両制御装置のためのメモリ書き換えシステムにおいて、第2のセキュリティ情報の書き込みプログラムによって実行され、該プログラムが、前記車両制御装置に搭載された消去および書き込みが不可能なメモリ領域に格納されているという構成をとる。

【0016】請求項2の発明によると、セキュリティ情報を書き換えるプログラムが、変更不能なメモリに格納されており、第三者によって改ざんされることはないので、安心してセキュリティ情報の書き換えを実行することができる。

【0017】請求項3の発明は、請求項1または請求項2の車両制御装置のためのメモリ書き換えシステムにおいて、第2のセキュリティ情報が、書き換え装置によって任意に設定されるという構成をとる。

【0018】請求項3の発明によると、書き換え装置によって任意に新たなセキュリティ情報を設定することができるので、第三者に知られることなく、柔軟性をもって新たなセキュリティ情報を設定することができる。

【0019】請求項4の発明は、請求項1から請求項3のいずれかの車両制御装置のためのメモリ書き換えシステムにおいて、第1のセキュリティ情報による書き換え許可が、盗難防止システムによって車両動作が許可された場合に書き換えが許可されるという構成をとる。

【0020】請求項4の発明によると、盗難防止システムが車両動作を許可したことを条件にメモリの書き換えが実行されるので、不正な運転者による書き換えを防止することができ、よって盗難防止システムに関する情報の書き換えを防止することができる。

【0021】

【発明の実施の形態】次に図面を参照してこの発明の実施の形態を、車両制御装置の不揮発性メモリに格納されたセキュリティプログラムを書き換えるシステムに関して説明する。しかし、この発明は、セキュリティプログラムを書き換えるシステムに限定されるものではなく、広く不揮発性メモリに格納された情報を書き換えるシステムに適用することができる。

【0022】図1は、この発明によるメモリ書き換えシステムの概要を示す。メモリ書き換えシステムは、車両1に搭載された電子制御ユニット(ECU)10および書き換え装置11を備える。書き換え装置11は、車両1のメーカーによって認可された正規の書き換え装置である。ECU10は、消去および書き込み可能なROM(図示せず)を備えている。図に示されるように、書き換え装置11をECU10に接続し、書き換え装置11を操作することにより、ECU10のROMに格納されたプログラムおよびデータのような情報が不正に書き換えられることを防止するセキュリティを解除し、該ROMに格納された情報を書き換えることができる。

【0023】書き換えは、ECU10および書き換え装置11の間のシリアル通信を介して行われる。書き換え装置11を操作するユーザーは書き換え装置11のボタンを操作し、書き換え装置11に備えられた表示画面と対話しながら、書き換える情報をECU10に送信することができる。しかし、書き換え装置は、図に示されるような形態に限定されるものではなく、シリアル通信を介してECU10と通信するプロトコルを持つ他の形態の装置を書き換え装置として使用するようにしてもよい。

【0024】図2は、この発明に従うメモリ書き換えシステムの全体的な機能ブロック図を示す。前述したように、メモリ書き換えシステムは、車両に搭載されたECU10および書き換え装置11を備える。書き換え装置11はECU10の外部に設けられ、ECU10とシリアル通信を介して接続される。なお、書き換え装置11およびECU10の間の通信をパラレル通信によって実現することも可能である。

【0025】ECU10は、マイクロコンピュータおよびこれに付随する回路素子で構成され、中央演算処理装置14（以下「CPU」という）、不揮発性メモリであって、実行するプログラムおよびデータを格納するROM16および18、実行時の作業領域を提供し演算結果などを記憶するRAM37（ランダムアクセスメモリ）、各種センサ39からの信号を受け取り、車両の各部に制御信号を送る入出力インターフェース38を備える。各種センサ39からの信号には、エンジン回転数（Ne）、エンジン水温（Tw）、吸気温（Ta）、バッテリー電圧（VB）、イグニションスイッチ（IGSW）などが含まれる。こうして、CPU14は、入出力インターフェース38から入力された信号に基づいて、ROM16および18から制御プログラムおよびデータを呼び出して演算を行い、その結果を入出力インターフェース38を介して車両の各部に出力し、車両の様々な機能を制御する。

【0026】また、ECU10は、インターフェース12を備える。インターフェース12は、書き換え装置11との通信のプロトコルを持ち、ECU10および書き換え装置11の間のシリアル通信を可能にする。

【0027】変更可能ROM16は、格納された情報を消去して書き込むことができるメモリであり、たとえばフラッシュメモリ、EEPROMによって実現することができる。変更不可能ROM18は、上記のフラッシュメモリ、EEPROMのような消去および書き込み可能なROMのメモリ領域のうち、ある領域を変更不可能領域と設定することによって実現することができ、または製造時にデータが決められ、その後に消去および書き込みができないマスクROMや、または1度だけデータを書き込むことができるPROMなどによっても実現することができる。

【0028】これらのROM16および18は、別個のメモリとして実現してもよく、または1つのメモリのメモリ領域を2つの領域に分割して一方を変更可能領域として使用し、他方を変更不可能領域として使用することもできる。後者の場合、たとえばEEPROMのある特定の領域を変更不可能領域としてプログラムなどを格納した後、それ以外の空き領域に対してスタートおよびエンドアドレスを指定することにより、変更可能領域を設定することができる。

【0029】ここで、ROM16、18およびCPUの実現の形態例について、図3を参照する。図3においては、ROM16および18はフラッシュメモリによって実現される。図3の（a）は、フラッシュメモリがCPUと別個に設けられた形態を示す。書き換え装置との通信により書き換えモードに移行すると、CPUは、書き換え装置からプログラムコードを受信し、書き換えを実行するプログラムを呼び出して、受信したプログラムコードをフラッシュメモリに書き込む。

【0030】一方、図3の（b）は、フラッシュメモリが内蔵されて、CPUと共に1チップを構成する形態を示す。書き換え装置からの信号によって書き換えモードに移行すると、書き換え装置からのプログラムコードは、CPUに組み込まれた機能によって自動的にフラッシュメモリに書き込まれる。いずれの形態においても、この発明によるメモリ書き換えシステムを適用することができる。

【0031】図2に戻ると、変更可能ROM16にはセキュリティ関数 $f_2$ が格納されており、この関数 $f_2$ が、書き換え装置11による書き換えの対象となる。セキュリティ関数 $f_2$ は、ROM16に格納された情報が不正に書き換えられることを防止するセキュリティ機能を実現する関数である。

【0032】変更不可能ROM18には、認証部31、乱数生成部33および書き換え実行部35を実現するプログラムが格納される。認証部31は、書き換え装置11からのセキュリティ解除要求に応答して、セキュリティ関数 $f_2$ および乱数Rを使用し、書き換え装置11が正規の書き換え装置かどうかを判断する。乱数Rを使用するのは、セキュリティ機能を向上させるためであり、乱数Rは、乱数生成部33により生成される。正規の書き換え装置と判断したならば、セキュリティを解除する。書き換え実行部35は、認証部31によりセキュリティが解除された後、セキュリティ関数 $f_2$ を消去し、書き換え装置11から新たなセキュリティ関数 $f_3$ を受信して、それをROM16に書き込む。

【0033】書き換え装置11は、セキュリティ関数 $f_1$ および新たなセキュリティ関数 $f_3$ を持つ。セキュリティ関数 $f_1$ は、上記のROM16に格納されたセキュリティ関数 $f_2$ と対になってセキュリティ機能を実現する関数である。セキュリティ関数 $f_2$ が第三者によって

変更されていなければ、書き換え装置11の持つセキュリティ関数 $f_1$ およびECU10の持つセキュリティ関数 $f_2$ は、同じ関数である。代わりに、セキュリティ関数 $f_1$ および $f_2$ の間に何らかの一定の関係を持たせるようにしてもよい。

【0034】新たなセキュリティ関数 $f_3$ は、新たなセキュリティ機能を実現するものとして、セキュリティ関数 $f_2$ の代わりにROM16に格納されることになる関数である。新たなセキュリティ関数 $f_3$ は、現在のセキュリティ関数 $f_1$ および $f_2$ に何らかの変更を加えたものであり、たとえば関数の式自体が異なったもの、または関数に含まれる定数を変更したものでよい。たとえば、関数 $f_1$ および $f_2$ が、 $f_1 = f_2 = A \times R + B$ （ここで、 $A = 10$ 、 $B = 5$ ）であるとき、新たなセキュリティ関数 $f_3$ を $f_3 = A + R \times B$ （ここで、 $A = 10$ 、 $B = 5$ ）のように設定することができる。または、 $f_1$ および $f_2$ の定数 $A$ および $B$ の値を、 $A = 5$ 、 $B = 10$ のように変更することもできる。

【0035】書き換え装置11は、セキュリティ解除要求部21、書き換え要求部23、データ列組立部25を備え、これらはプログラムとして書き換え装置11のメモリに格納されている。セキュリティ解除要求部21は、セキュリティ関数 $f_1$ を使用して、ECU10に対してセキュリティ解除を要求する。

【0036】データ列組立部25は、ECU10に送信される新たなセキュリティ関数 $f_3$ のプログラムコードを、シリアル通信に適したデータ列に組み立てる。たとえば、データ列組立部25は、セキュリティ関数 $f_3$ のプログラムを、ある長さのプログラムコード（たとえば、8ビット）に分割して、シリアル通信に適したシリアルデータ列の形式に変換する。その時、それぞれのプログラムコードには、プログラムコードが格納される先頭アドレスを含むアドレスフィールドが付加される。こうして、それぞれのプログラムコードがECUに転送されたとき、該プログラムコードがメモリのどの場所に格納されるべきかをECUに知らせるようにする。

【0037】書き換え要求部23は、セキュリティが解除された後に、データ列組立部25によって組み立てられた新たなセキュリティ関数 $f_3$ を表すデータ列をECU10に送信する。

【0038】ECU10には盗難防止システム81が接続されており、メモリ書き換えシステムは、盗難防止システム81と情報を交換することができる。盗難防止システム81は、エンジン始動の際にキーシリンダに挿入されたイグニッションキーから、該キーに含まれる電子コードを抽出し、該電子コードと予め設定された正規のコードとを比較して、挿入されたイグニッションキーが正規のものかどうか判断する。イグニッションキーが正規のものか判断されたならば、盗難防止システム81は、エンジン始動許可を示す信号を入出力インターフェース38

を介してECU10に送信する。ECU10は、エンジン許可信号の受信に応答して、エンジンを始動させることができる。

【0039】挿入されたイグニッションキーが正規のものと判断されなければ、エンジン始動許可信号は出力されず、ECU10はエンジンを始動させることができない。ECU10に送信されたエンジン始動許可信号により、RAM37（またはROM16）に格納されたエンジン始動許可フラグに値1が設定される。図2では別々に書かれているが、盗難防止システム81の機能の一部をECU10に含めることができる。たとえば、正規のイグニッションキーかどうかの判断を、ECU10によって実行するようにしてもよい。

【0040】図2に示されるメモリ書き換えシステムの動作の概要を、図4および図5を参照しながら説明する。書き換え装置11をECU10に接続した後、書き換え装置11のたとえば何らかの操作ボタンを押すことにより、書き換え動作が開始する。または、ECUを操作して、書き換え動作を開始するようにしてもよい。

【0041】ステップ41において、書き換え装置11のセキュリティ解除要求部21は、ECU10にセキュリティ解除要求信号を送信する。ECU10は、それに応答して、正規の書き換え装置が接続されていることを確認する認証処理を開始する。

【0042】認証処理の一例を図5に示す。ステップ51において、書き換え装置11のセキュリティ解除要求部21は、任意の数 $R$ を送信するようECU10に要求する。それに応答して、ECU10の認証部31が呼び出される。認証部31は、乱数生成部33を呼び出して、乱数によって任意の数 $R$ を設定し、その任意の数 $R$ を書き換え装置11に送信する（ステップ52）。なお、上記の乱数を使用して数 $R$ を設定する代わりに、異なる機構を用いて任意に数 $R$ を設定するようにしてもよい。書き換え装置11は、予め内部に持っているセキュリティ関数 $f_1$ を使用して、 $K1 = f_1(R)$ により、数 $R$ に対する関数 $f_1$ の関数値 $K1$ を求める（ステップ53）。

【0043】一方、ECU10の認証部31は、変更可能ROM16に格納されたセキュリティ関数 $f_2$ を使用して、 $K2 = f_2(R)$ を計算して関数値 $K2$ を求める（ステップ54）。書き換え装置11のセキュリティ解除要求部21は、関数値 $K1$ をECU10に送信する（ステップ55）。認証部31は、書き換え装置11からの関数値 $K1$ と、内部で生成した関数値 $K2$ を比較し（ステップ56）、一致したならば、正規の書き換え装置と判断する。続いて、認証部31は、RAM37に格納されたエンジン始動許可フラグに値1が設定されているかどうか調べる（ステップ57）。許可フラグに値1が設定されていれば、盗難防止システム81からエンジン始動許可信号が出力されたことを意味するので、書き

換え許可信号を書き換え装置11に送信する(ステップ58)。このように、書き換えを実行するには、まずセキュリティを解除する必要がある。現在のセキュリティ関数 $f_1$ および $f_2$ を使用して、セキュリティを解除する。盗難防止システムが搭載されている場合には、盗難防止システムの解除を条件にメモリ書き換えシステムのセキュリティを解除するので、不正な運転者による書き換えおよび盗難防止システムに関する情報の書き換えを防止することができる。

【0044】図4に戻り、ECU10によって書き換え装置11が正規のものであると認証されて書き換えが許可されたならば、ステップ42に進む。書き換え装置11の書き換え要求部23は、書き換え開始信号をECU10に送り、ECU10の書き換え実行部35は、準備ができたならば、開始許可信号を返す。ステップ43において、書き換え装置11は、書き換え動作モードに移行する要求をECU10に送り、ECU10の書き換え実行部35は動作モード移行処理を行う。ステップ44において、書き換え要求部23は動作モードの移行が完了したかをECU10に問い合わせ、書き換え実行部35は、動作モードの移行が完了したならば、移行完了信号を書き換え装置11に送信する。

【0045】ステップ45において、書き換え要求部23は、変更可能ROM16に格納されたセキュリティ関数 $f_2$ の消去を要求し、書き換え実行部35は応答して、ROM16のセキュリティ関数 $f_2$ を消去する。

【0046】書き換え装置11においては、新たなセキュリティ関数として関数 $f_3$ が設定され、データ列組立部25によって、この新たなセキュリティ関数 $f_3$ は、ECU10に送信するためのシリアルデータ列として準備されている。このセキュリティ関数 $f_3$ の設定およびそのデータ列の組立は、通常、書き換え装置11によってセキュリティ解除要求または書き換え開始信号をECU10に送信する前に行われる。しかし、ステップ45の直前に行うようにしてもよい。

【0047】セキュリティ関数 $f_3$ は、たとえば書き換え装置11に予め保存されているいくつかの関数の中から選択することによって設定することもでき、またはユーザーが書き換え装置11を操作しながら新たな関数を作成するようにしてもよい。

【0048】ステップ46において、書き換え要求部23は、書き込み要求信号と共に、新たなセキュリティ関数 $f_3$ を表すデータ列をECU10に送信する。書き換え実行部35は、書き換え装置11からデータ列を受信し、該データ列に含まれるプログラムコードを変更可能ROM16に書き込む。書き込みを完了すると、書き換え実行部35は、書き込み完了通知を書き換え装置11に送信する。書き換え装置11は、それに応答して、次のデータ列をECU10に送信する。このステップ46は、ROM16に、セキュリティ関数 $f_3$ のすべてのプ

ログラムコードの書き込みが完了するまで繰り返される。

【0049】書き込みが完了したならば、書き換え要求部23は、書き換え動作モードを解除する要求をECU10に送信する(ステップ47)。書き換え実行部35は、それに応答して書き換え動作モードを解除する。書き換え装置11によって、ROM16に格納されたセキュリティ関数が $f_3$ に変更されたので、書き換え装置11で使用されるセキュリティ関数も $f_3$ に設定され、その後のセキュリティ機能は、セキュリティ関数 $f_3$ によって実現される。新たなセキュリティ関数 $f_3$ を設定した後、または新たなセキュリティ関数 $f_3$ をROM16に書き込んだ後、前のセキュリティ関数 $f_1$ を消去することができる。

【0050】図6は、書き換え装置で実行される、セキュリティ解除の手順を示すフローチャートである。ステップ61において、書き換え装置は、ECUに対して数Rを要求する。その後、書き換え装置は、ECUから任意の数Rを受信する(ステップ62)。数Rを受信したならば、予め内部に持っているセキュリティ関数 $f_1$ を使用して、数Rに対する関数値K1を計算する(ステップ63)。その後、関数値K1をECUに送信する(ステップ64)。

【0051】図7は、ECUで実行される、セキュリティ解除の手順を示すフローチャートである。ステップ71において、ECUは、書き換え装置からの数Rの要求を受信する。受信したならば、乱数を使用してRを設定し(ステップ72)、数Rを書き換え装置に送る(ステップ73)。その後、ECUは、内部に持っているセキュリティ関数 $f_2$ を使用して、数Rに対する関数値K2を計算する(ステップ74)。

【0052】ECUは、書き換え装置から関数値K1を受信し(ステップ75)、K1およびK2を比較する(ステップ76)。一致したならば、エンジン始動許可フラグに値1が設定されているかどうか調べる(ステップ77)。値1が設定されていれば、ステップ78に進んで書き換え許可フラグに1を設定し、書き換え装置による書き換えが許可されたことを示す。ステップ76において一致しなければ、またはステップ77においてエンジン始動許可フラグに値1が設定されていなければ、書き換え許可フラグにゼロを設定して(ステップ79)、この書き換え装置によっての書き換えは許可されないことを示し、処理を中止する。

【0053】図8は、書き換え装置で実行される、書き換え手順を示すフローチャートである。ステップ81において、書き換え装置は、書き換え要求をECUに送信する。この書き換え要求は、実際には図4に示されるように、書き換え開始の通知、書き換え動作モードへの移行要求などを含むことができる。書き換え要求に対するECUの許可応答を受信したならば(ステップ82)、



設定された新たなセキュリティ関数 $f_3$ のデータ列を作成する(ステップ83)。新たなセキュリティ関数 $f_3$ は、前述したように、書き換え装置を使用して任意に設定することができる。その後、新たなセキュリティ関数 $f_3$ を表すデータ列を、ECUに送信する(ステップ84)。

【0054】図9は、ECUで実行される、書き換え手順を示すフローチャートである。書き換え装置から書き換え要求を受信したならば(ステップ91)、書き換え許可フラグが1に設定されているかどうか調べる(ステップ92)。1に設定されているならば、正規の書き換え装置として認証されたことを示すので、書き換え装置から転送される新たなセキュリティ関数 $f_3$ を待つ。実際には、ステップ92および93の間には、図4に示されるように、書き換え動作モードへの移行、変更可能ROMの現在のセキュリティ関数 $f_2$ の消去などの処理を実行することができる。

【0055】その後、新たなセキュリティ関数 $f_3$ を受信したならば(ステップ93)、変更可能ROMに、この新たなセキュリティ関数 $f_3$ を書き込む。こうして、変更可能ROMに格納されていたセキュリティ関数 $f_2$ が、セキュリティ関数 $f_3$ に書き換えられる。

【0056】

【発明の効果】請求項1の発明によると、車両制御装置のメモリに記憶された情報が不正に書き換えられることを防止する書き換え許可を判断するセキュリティ情報が第三者に知られてしまった場合でも、書き換え装置によりこのセキュリティ情報を変更することができるので、不正なメモリ書き換えの拡大を防止することができる。

【0057】請求項2の発明によると、セキュリティ情報を書き換えるプログラムが、変更不可能なメモリに格納されており、第三者によって改ざんされることはないので、安心してセキュリティ情報の書き換えを実行することができる。

【0058】請求項3の発明によると、書き換え装置によって任意に新たなセキュリティ情報を設定することができるので、第三者に知られることなく、柔軟性をもつ

て新たなセキュリティ情報を設定することができる。

【0059】請求項4の発明によると、盗難防止システムが車両動作の許可をしたことを条件にメモリ書き換えが実行されるので、不正な運転者による書き換えを防止することができ、よって盗難防止システムに関する情報の書き換えを防止することができる。

【図面の簡単な説明】

【図1】この発明に従うメモリ書き換えシステムの概要を示す図。

【図2】この発明の一実施例における、メモリ書き換えシステムの全体を示すブロック図。

【図3】この発明の一実施例における、メモリ書き換えシステムのECUのROMおよびCPUの形態例を示す図。

【図4】この発明の一実施例における、メモリ書き換えシステムの動作手順を示す図。

【図5】この発明の一実施例における、メモリ書き換えシステムの認証手順を示す図。

【図6】この発明の一実施例における、メモリ書き換えシステムの書き換え装置で実行されるセキュリティ解除の手順を示すフローチャート。

【図7】この発明の一実施例における、メモリ書き換えシステムのECUで実行されるセキュリティ解除の手順を示すフローチャート。

【図8】この発明の一実施例における、メモリ書き換えシステムの書き換え装置で実行される書き換え手順を示すフローチャート。

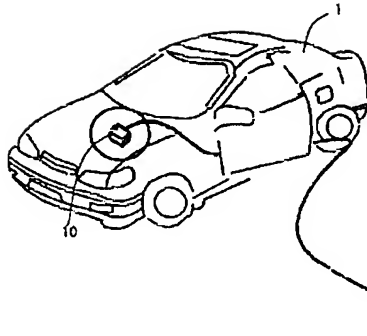
【図9】この発明の一実施例における、メモリ書き換えシステムのECUで実行される書き換え手順を示すフローチャート。

【符号の説明】

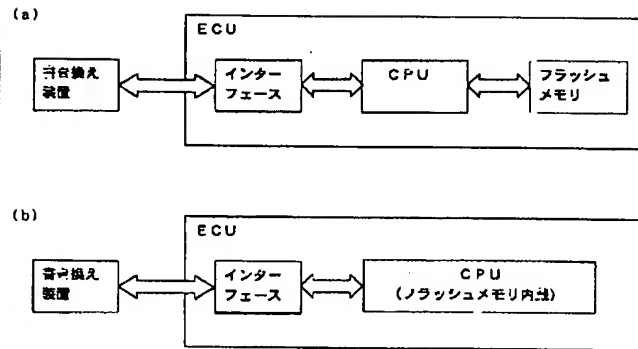
|    |          |    |          |
|----|----------|----|----------|
| 10 | ECU      | 11 | 書き換え装置   |
| 12 | インターフェース | 14 | CPU      |
| 16 | 変更可能ROM  | 18 | 変更不可能ROM |
| 81 | 盗難防止システム |    |          |



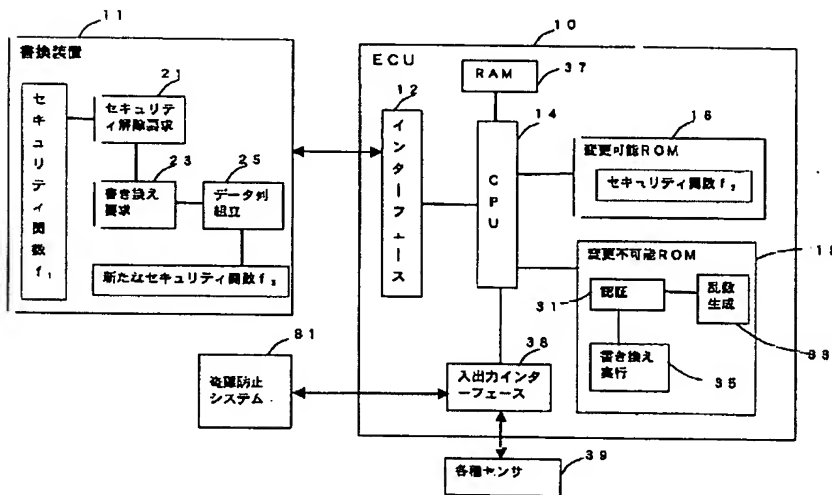
【図1】



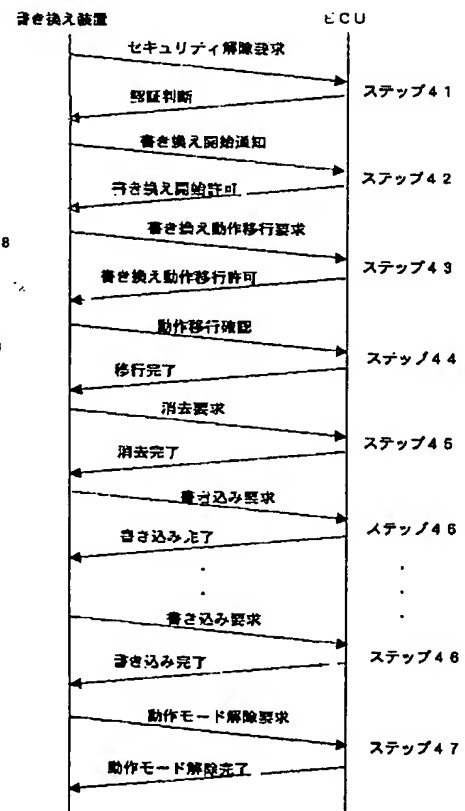
【図3】



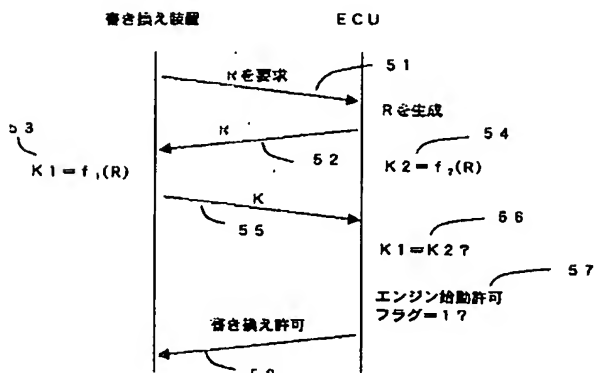
【図2】



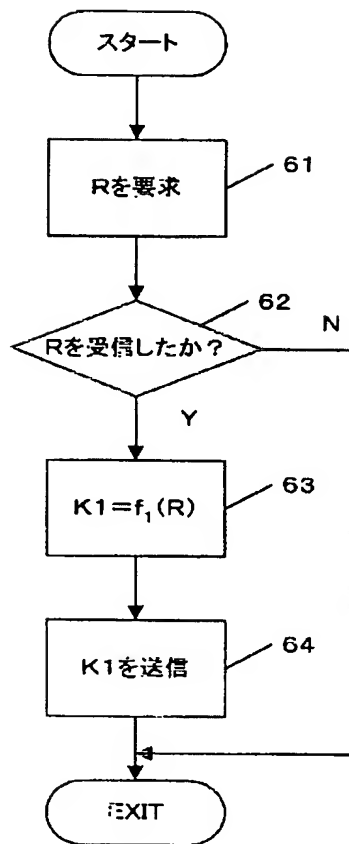
【図4】



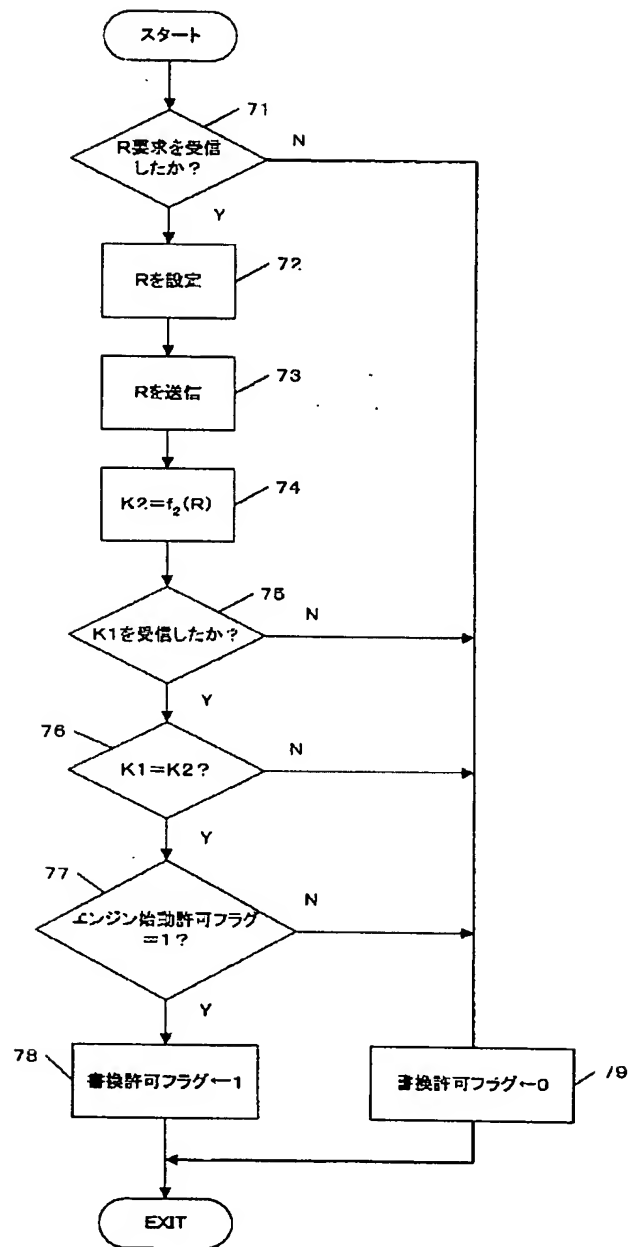
【図5】



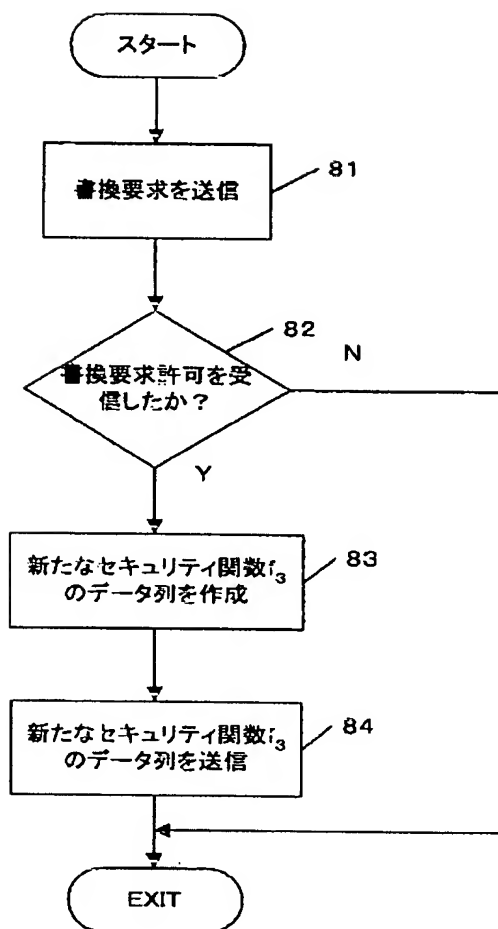
【図6】



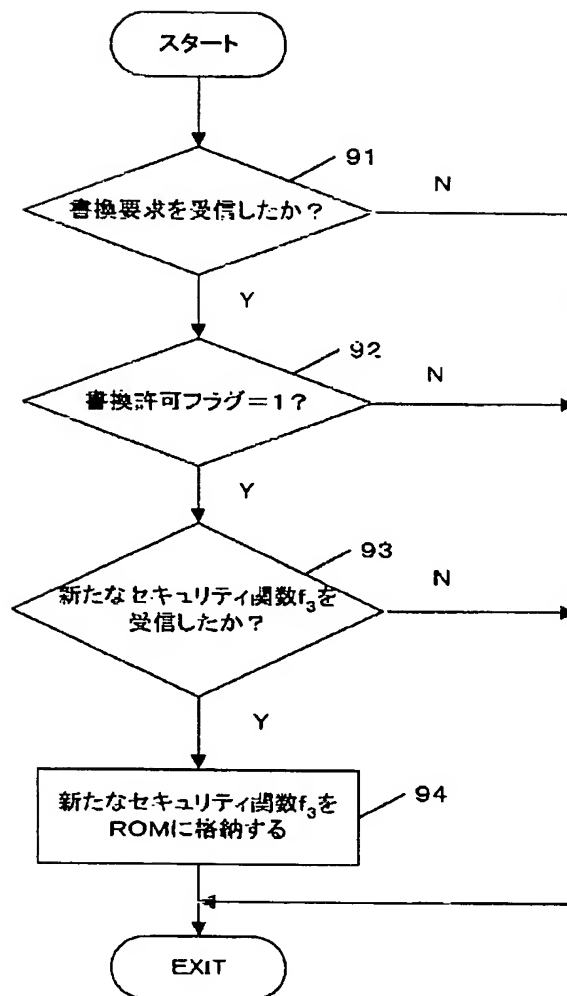
【図7】



【図8】



【図9】



フロントページの続き

(72)発明者 水尾 直彦  
埼玉県和光市中央1丁目4番1号 株式会  
社本田技術研究所内

Fターム(参考) 5B017 AA02 BA02 CA15  
5B076 EB01 FA07